Observatoire du Monde Cybernétique
Trimestriel

Mars 2014

Système de réseaux

CYBERESPACE

Cyberconflit

Données

Lutte informatique

Infoguerre

Cyber warfare

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE



La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Sommaire

1. Capacités de lutte informatique russes : état des lieux

Les capacités de lutte informatique russes sont le fruit d'une construction historique unique, marquée par la prépondérance des services secrets et la chute de l'URSS. Depuis la fin du vingtième siècle, ces capacités ont été utilisées en plusieurs occurrences et à grande échelle. Si la Russie reste très discrète quant à l'étendue des moyens consacrés au cyber, il convient de rappeler que le général Alexander annonçait dès 2010, année de la création du US Cyber Command, que les capacités de lutte informatique russes étaient proches de celles des Etats-Unis.

L'opération Moonlight Maze de 1999, les attaques par déni de service distribué (DDoS) massives contre les sites gouvernementaux estoniens et géorgiens en 2007 et 2008, ou encore celles en cours bloquant les téléphones des parlementaires ukrainiens, sont autant d'exemples montrant l'étendue des capacités de lutte informatique russes et la facilité avec laquelle les autorités peuvent décider de les employer. Ces attaques, sur lesquelles nous reviendrons en détail, démontrent que la Russie a à sa disposition une grande variété de modes d'action dans le cyber qu'elle choisit d'utiliser en fonction des objectifs à atteindre.

Ainsi, début 2014, la Russie apparaît comme le pays ayant eu le plus recours à des cyberattaques massives dans des situations pourtant très différentes.

Il convient dans un premier temps d'étudier la construction historique des capacités de lutte informatique russes, afin de comprendre ensuite les modes d'action et les conditions d'emploi des forces cyber russes dans les conflits actuels.

1.1 Une construction historique unique des capacités de lutte informatique

Les capacités cyber russes sont le fruit d'une construction historique entamée sous l'URSS et marquée à la fois par la rupture qu'a constitué la chute de l'union soviétique, et la prégnance continue des services secrets russes.

1.1.1 *Des technologies sous contrôle et tenues secrètes*

L'informatique a connu un fort développement sous l'URSS pour plusieurs raisons[1] : l'impossibilité de procéder à des échanges technologiques avec les occidentaux, la nécessité de disposer de technologies - parmi lesquelles les supercalculateurs - essentielles à la course à l'armement contre les États-Unis, et la volonté de montrer que l'URSS pouvait dépasser les autres nations en développement technologique. Le développement des supercalculateurs reflète bien les performances soviétiques en matière d'informatique. Dès 1953, Sergeï Alexeïevitch Lebedev est parvenu à mettre au point le premier supercalculateur BESM, ce qui représentait alors un véritable « tour de force »[2] technologique.

Cependant, ces avancées n'ont que peu bénéficié à la société civile du fait du secret qui les entourait. Si les autorités soviétiques annonçaient parfois une percée technologique majeure dans ce domaine afin de montrer que l'union soviétique pouvait faire jeu égal avec ses rivaux, ces avancées étaient généralement tenues secrètes du fait de leur rôle stratégique et de la volonté de ne pas attirer l'attention sur ce domaine. Cette importance du secret s'est maintenue bien après la chute de l'URSS comme l'illustrent les restructurations de l'université Voronez en 2006 puis 2009. En 2006, le Voronezh Military Radio-electronics Institute a fusionné avec la Voronezh Aviation Engineering School pour former la Voronezh Aviation Engineering University[3]. En 2008, le président Vladimir Poutine a signé l'ordre de la Fédération de Russie n°51 initiant une nouvelle restructuration de l'école récemment créée. Celle-ci aurait intégré au moins deux départements tenus secrets et dédiés à la sécurité de l'information et la guerre de l'information, dont les ressources pourraient être utilisées dans le cadre de la crise en Ukraine[4]. La communication autour de cette école diffère de celle des autres pays, parmi lesquels le Brésil ou la France, qui annoncent officiellement leurs créations.

---

[1] Yannick Harrel, La Cyber Stratégie Russe, 2013
[2] Yannick Harrel, La Cyber Stratégie Russe, 2013
[3] http://jeffreycarr.blogspot.fr/2014/03/does-voronezh-military-hacking-school.html
[4] http://jeffreycarr.blogspot.fr/2014/03/russia-v-ukraine-exploring-cyber-side.html

Le contrôle et le secret entourant l'informatique a eu d'importantes conséquences après la chute de l'URSS. De nombreux ingénieurs informatiques ont alors perdu leur emploi et se sont trouvés dans l'incapacité de continuer leurs travaux ou de faire valoir leur niveau d'expertise dans une société civile n'ayant pas bénéficié des avancées technologiques étatiques. Cet état de fait a mené à deux tendances : **la constitution de réseaux de cybercriminels ayant une forte expertise en informatique, et une « *fuite des cerveaux* » vers d'autres pays susceptibles d'embaucher les jeunes chercheurs et ingénieurs.**

1.1.2 *Le poids des services secrets dans le milieu « cyber » russe*

Les services secrets ont joué un rôle important dans le développement des capacités cyber russes, ainsi que dans leur contrôle. La collecte de renseignement sur les technologies dans les pays tiers a favorisé les avancées technologiques dans tous les secteurs en URSS, et contribué à la course à l'armement et potentiellement au développement de l'informatique. Avant 1991, le KGB avait commencé à s'intéresser aux possibilités d'action qu'ouvraient le cyberespace et les technologies. Un des éléments les plus importants en termes de prise de conscience est le sabotage d'un pipeline en Sibérie par le biais d'une cyberattaque. Comme le relate Thomas Reed[5], la CIA aurait réussi à se procurer la liste des logiciels que Moscou cherchait à acquérir pour mettre à jour la gestion de ses pipelines et aurait piégé les autorités russes en les faisant acheter un logiciel volontairement défectueux. Celui-ci était programmé pour produire des niveaux de pression bien au-dessus de ce que le pipeline pouvait supporter et ainsi le faire exploser comme ce fut le cas en 1982[6].

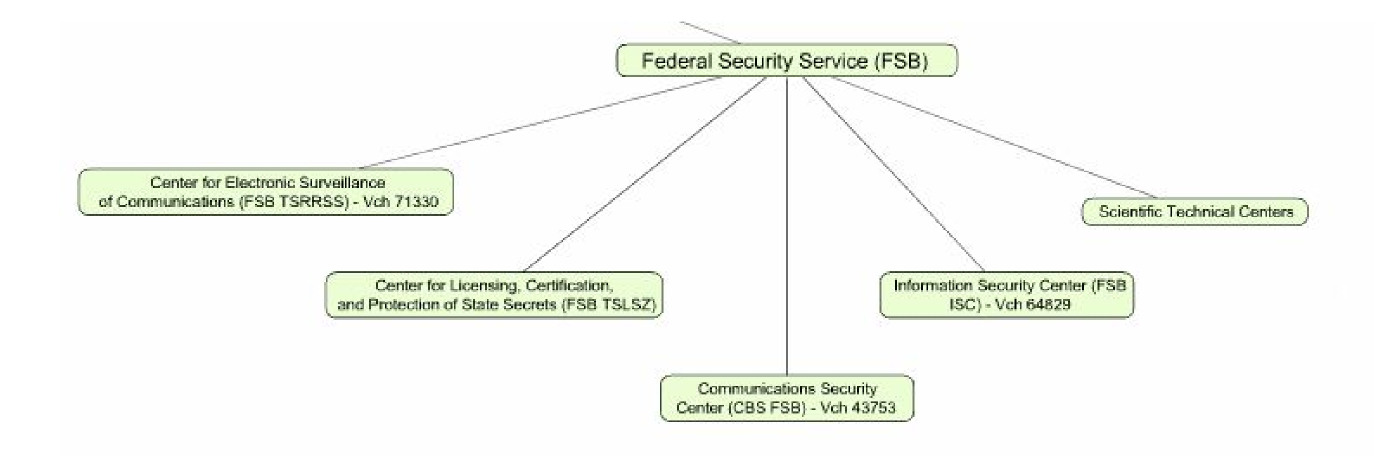
La chute de l'URSS en 1991 a marqué un coup d'arrêt dans le bon fonctionnement des services secrets russes, ainsi que dans leur développement de capacités cyber, Cependant, le FSB a rapidement repris la main sur les opérations de surveillance de masse sur le territoire national et à l'étranger. En effet, si le FSB est principalement engagé dans les affaires intérieures, il inclut également en son sein le Service Fédéral des communications et informations gouvernementales (FAPSI)[7] qui est en charge de la surveillance des communications à l'étranger.

---

[5]Thomas Reed, At the Abyss: An Insider's History of the Cold War, 2005

[6]http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html

[7]https://www.privacyinternational.org/blog/lawful-interception-the-russian-approach



Composantes cybersécurité du FSB[8]

Dans cette optique, le FSB dispose de moyens d'interception des communications téléphoniques ou par Internet éprouvés, dans le cadre du programme SORM. Ce système, dont la première version a été lancée en 1996 afin de surveiller les communications téléphoniques, a été étendu à Internet en 1998 et constamment amélioré depuis. Une loi de 2000 a obligé les fournisseurs d'accès à Internet à installer un dispositif sur leurs serveurs permettant au FSB d'accéder à tout moment aux données relatives à un utilisateur. La version actuelle, SORM 3, stocke les données relatives à toute forme de communication. La surveillance d'Internet est un élément très important pour les capacités cyber russes[9]. Elle connaît un développement permanent et joue un rôle structurant dans la lutte informatique russe (*cf. infra)*.

1.1.3 *Une cybercriminalité au profil particulier*

Les chercheurs et ingénieurs en informatique sont pour beaucoup devenus sans emploi à la chute de l'URSS. Une partie d'entre eux ont rejoint des réseaux cybercriminels, tout en restant bien connus des services de renseignement du fait de l'importance stratégique de leurs travaux passés. Ces réseaux cybercriminels, coordonnés par la mafia, ont gagné en puissance sans être inquiétés par les autorités russes. Parmi les réseaux de cybercriminels, le plus connu est le *Russian Business Network (RBN)*. Ce groupe, créé en 2004, est notamment suspecté d'avoir entretenu un réseau de machine infecté du nom de Storm qui a été découvert en 2007[10]. Si le nombre de machines infectées constituant le réseau est variable et n'a pas été défini précisément, des experts informatiques estiment que celui-ci comptait entre 160 000 et 1 million d'ordinateurs zombies[11].

[8]http://prezi.com/ajo61qec9rwi/russian-cyber-security-organization/
[9]http://www.worldpolicy.org/journal/fall2013/Russia-surveillance
[10]http://rbnexploit.blogspot.fr/2008/02/rbn-extortion-and-denial-of-service.html
[11]http://www.journaldunet.com/solutions/securite/actualite/07/1029-storm-botnet-contre-attaque.shtml

1.2 Atouts et modes d'action des forces cyber russes

Les cyberattaques massives sont plus efficaces dans le voisinage immédiat de la Russie. Cette dernière possède en effet un renseignement d'intérêt cyber de qualité dans les pays voisins. Celui-ci décuple les capacités de lutte informatique russes qui reposent sur des relations informelles avec les réseaux de cybercriminels et une lutte informatique militaire qui se structure officiellement.

1.2.1 *Des capacités « régionalisées » par un renseignement d'intérêt cyber orienté*

Du fait de l'héritage soviétique en termes d'infrastructures et réseaux télécoms, de technologies utilisées et de collaboration entre services, la Russie possède une très bonne connaissance des cibles potentielles dans son environnement géographique immédiat. Ce renseignement d'intérêt cyber, décuplé par des capacités de renseignement humain historiquement fortes, permet à la Russie de mener avec plus de facilité des cyberattaques massives qui pourraient difficilement avoir lieu dans des pays plus éloignés et moins connus des autorités russes.

Ce renseignement d'intérêt cyber se décompose en au moins trois éléments. Tout d'abord, la Russie dispose d'une très bonne connaissance de la structure des réseaux télécoms des pays ayant fait partie de l'URSS. Cela lui permet de visualiser les points faibles du réseau, ainsi que le fonctionnement des opérateurs principaux qui se sont construits sur une structure héritée de l'union soviétique. Ensuite, la Russie dispose également d'un très bon renseignement humain dans ces pays. A des fins cyber, ce renseignement facilite l'accès à des réseaux protégés en exploitant la faille *« humaine »*, et collecte des informations sur les technologies utilisées afin de préparer des cyberattaques.

Enfin, les transferts de technologie entre la Russie et les pays de la région, notamment dans le cadre de la collaboration entre services de renseignement, constituent également un atout pour la préparation de cyberattaques. Le système russe de surveillance de masse des communications, SORM, a par exemple été mis en place par au moins cinq pays de la Communauté des Etats Indépendants : l'Ukraine, la Biélorussie, l'Ouzbékistan, le Kirghizistan et le Kazakhstan. Au-delà du transfert de technologies, le KGB avait fixé dans les années 1960 les règles et les pratiques à mettre en place dans le cadre de la surveillance des communications. Une influence normative du FSB a potentiellement pu continuer à s'exercer à la chute de l'URSS, donnant à la Russie une connaissance des processus et des technologies utilisées par les services de renseignement étrangers.

La crise récente en Ukraine et ses implications cyber (*cf. infra*) illustrent bien l'importance du renseignement d'intérêt cyber russe dans son voisinage. Tout d’abord, l’organisation et la structure du réseau télécom ukrainien sont bien connus des services russes qui ont aidé le pays à se doter

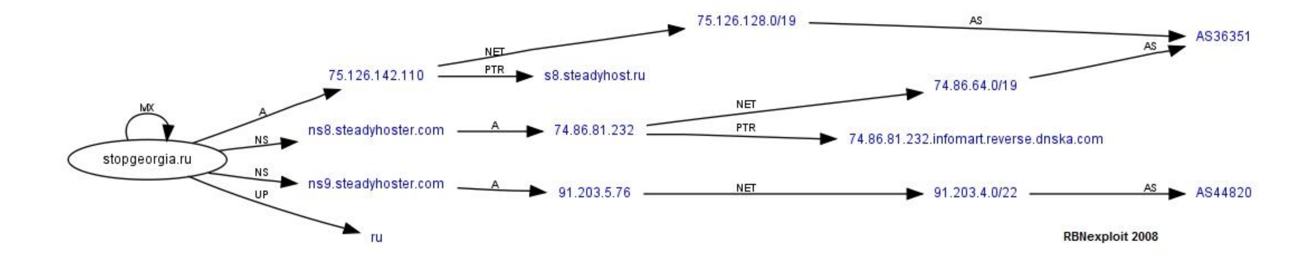
d'une capacité de surveillance de masse dès 2010[12]. L'Ukraine a adopté à cette époque SORM, un outil russe fourni par le FSB qui permet de surveiller les communications et d'accéder aux données contenues dans les serveurs situés sur son territoire. Il est possible d'imaginer que ce partenariat entre les services ukrainiens et russes, et l'adoption de technologies russes par l'Ukraine, a permis à la Russie d'accéder à une grande quantité d'informations relatives au réseau télécom ukrainien. De plus, la structure physique du réseau télécom ukrainien est d'autant plus facile à cartographier qu'elle est héritée de l'époque soviétique et est administrée par un seul opérateur, Ukrtelecom. Enfin, la Russie dispose de fortes capacités de renseignement humain et d'influence dans les administrations ukrainiennes, comme l'ont montré les défections en cascade de hautes autorités ukrainiennes, parmi lesquelles le chef d'état-major de la marine ukrainienne, depuis l'arrivée des troupes russes. Toutes ces informations, entre autres, font partie d'un renseignement ciblé d'intérêt cyber qui augmente les chances de succès de cyberattaques massives dans les pays d'ex-URSS.

1.2.2 *Les liens entre les réseaux cybercriminels et la lutte informatique*

Plusieurs réseaux de cybercriminels en Russie sont connus par les autorités russes du fait, entre autres, du passé de certains ingénieurs travaillant autrefois pour l'état. Ces mêmes autorités sont tolérantes par rapport aux activités de groupes de hackers majeurs qui se sont fait connaître lors d'opérations de grande envergure. L'exemple le plus probant est celui du Russian Business Network. Ce réseau, créé en 2004 comme fournisseur d'accès à Internet, est aujourd'hui soupçonné de contribuer à des activités illégales en hébergeant des sites Internet illégaux, en mettant à disposition des criminels des kits de piratage avec leur manuel d'utilisation régulièrement mis à jour[13] (tels que le Mpack) ou encore en entretenant des réseaux de Botnet tels que Storm. Malgré ces activités illégales très visibles, le réseau de cybercriminel n'a jamais été inquiété par les autorités russes. Cela pourrait s'expliquer par des liens existant entre les réseaux cybercriminels majeurs et les autorités cyber russes, notamment dans le cadre d'opérations de lutte informatique offensive ou d'espionnage industriel ciblé sur lesquels nous reviendrons. Le rôle du Russian Business Network dans le cadre du conflit géorgien en 2008 illustre bien cette potentielle proximité. La Géorgie a été frappée par des cyberattaques par déni de service distribué (DDoS) massives au moment du déclenchement de l'invasion russe, qui ont continué après le 12 août 2008 et l'annonce de la fin des hostilités par les autorités russes. Des experts informatiques[14] ont fait remonter la *« première frappe cyber »* à deux membres du Russian Business Network, Alexandre Boykov et Andrey Smirnov. Plus largement, les DDoS ont été facilitées par la publication d'un site Internet, stopgeorgia.ru, listant les cibles à attaquer pour tout hacker soutenant le gouvernement russe… site également hébergé par Russian Business Network.

---

[12]http://www.worldpolicy.org/journal/fall2013/Russia-surveillance
[13]Yannick Harrel, la Cyber Stratégie russe (2013), p80
[14]http://hostexploit.com/downloads/view.download/4/9.html



Les adresses IP permettent de retracer les liens entre stopgeorgia.ru et les ordinateurs du Russian Business Nework[15]*.*

Il semble que des réseaux de cybercriminels majeurs puissent être mobilisés ponctuellement pour appuyer la lutte informatique offensive russe. Cependant, si ce fut le cas en 2008, ces réseaux ont tendance à devenir plus discret alors que dans le même temps la Russie met en place des forces militaires dédiées à la guerre de l'information et aux opérations de lutte informatique. En cela, 2008 peut représenter un tournant pour la lutte informatique russe et un basculement de l'emploi de capacités cyber détournées[16] par le biais de réseaux de cybercriminels à la constitution de troupes dédiées à la guerre de l'information au sein des forces armées russes. Il convient cependant de noter que cela concerne les opérations de lutte informatique dans le cadre de conflits armés, tandis que les campagnes de cyber espionnage de grande ampleur menées par les cybercriminels russes se sont maintenues.

1.2.3 *L'emploi des capacités de lutte informatique dans le cadre d'une stratégie informationnelle*

Les opérations en Géorgie en 2008[17] ont souligné les déficiences des forces militaires russes en matière de guerre de l'information, qui inclut à la fois le domaine technique et le domaine psychologique lié à l'information. Ce constat a mené au développement de chacune de ces capacités, et à la mise en place d'un nouveau cadre pour une stratégie informationnelle globale.

1.2.3.1 Le contrôle de l'information et les opérations psychologiques

Les autorités russes ont pris conscience dès 1999 des menaces liées à Internet, et à la guerre de l'information qu'il leur fallait mener pour contrôler l'information dans ce nouvel espace. A cette époque, face à la difficulté à contrôler le contenu publié par les Tchétchènes sur Internet, Vladimir Poutine déclarait que *« nous avons abandonné ce champ de bataille [celui de la guerre de*

[15] http://rbnexploit.blogspot.fr/2008/10/rbn-russian-cyberwar-on-georgia.html
[16] http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf
[17] T. L. Thomas. "Russian Information Warfare Theory: The Consequences of August 2008", extrait de S. Blank et R. Weitz. The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald, Carlisle: US Army War College Strategic Studies Institute 2010

l'information] il y a quelques temps (…) mais nous rentrons dans le jeu à nouveau »[18]. Au-delà du champ de bataille, le contrôle de l'information est un élément important pour Moscou qui a régulièrement dénoncé sa manipulation par d'autres puissances pour déstabiliser des pays. Plus récemment, les manifestations de 2011 en Russie lors des élections à la Douma, ou l'utilisation de l'information dans le cadre des révolutions arabes ont vivement inquiété les autorités russes. La Russie a proposé le 12 septembre 2011 un code de conduite[19] international sur la sécurité de l'information qui démontre cette inquiétude. Également signé par la Chine, le Tadjikistan et l'Ouzbékistan, la proposition de résolution insiste sur la nécessité de contrôler l'information afin de protéger la stabilité intérieure des États.

Recognizing the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security.

(Extrait du code de conduite proposé par la Russie à l'Assemblée Générale des Nations Unies)[20]

La préparation des Jeux Olympiques de Sotchi qui se sont déroulés début 2014 révèle les avancées russes en matière de contrôle de l'information et opérations psychologiques. Tout d'abord plusieurs actions ont eu pour effet de renforcer le "soft power" russe sur Internet. Le fait d'accorder le droit d'asile à Edward Snowden, la libération de militants de Greenpeace et de membres des Pussy Riots ont eu un effet positif sur les hacktivistes, qui cherchent à décrédibiliser les gouvernements et faire entendre leurs revendications par le biais de cyberattaques lors d'événements majeurs. Afin de désamorcer ce type d'actions, les autorités ont cherché à montrer leur attachement à des valeurs défendues sur Internet alors que les protestations se concentraient sur la National Security Agency. La récente déclaration du gouvernement de vouloir discuter en ligne, avec les citoyens russes, de la nouvelle stratégie de cybersécurité nationale adoptée en 2013 s'inscrit dans cette volonté de transparence et d'ouverture sur Internet. Si ces opérations de "désamorçage" peuvent porter leurs fruits, plusieurs mesures ont également été prises afin de dissuader les hacktivistes ou tout leader d'opinion de porter atteinte au succès de l'événement. Le service de sécurité du Kremlin, le FSO, a ainsi chargé des informaticiens professionnels de mettre sous surveillance des blogueurs ainsi que de recueillir toutes les données en lien avec le contenu publié sur les blogs. Ces actions, normalement menées par le FSO, ont été externalisées afin de pouvoir être menées à plus grande échelle en prévision des Jeux Olympiques. Pour finir, les moyens de surveillance de masse par le biais de SORM jouent également un rôle central dans le contrôle de l'information.

---

[18] http://www.rferl.org/content/article/1092360.html
[19] http://content.netmundial.br/files/67.pdf
[20] http://content.netmundial.br/files/67.pdf

La sécurité de l'information dans le domaine psychologique n'est pas le seul fait de forces armées ou de services secrets, mais englobe une large gamme d'acteurs contribuant à la stratégie russe[21]:

“The personnel of the Information Troops should be composed of diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others... To construct information countermeasures, it is necessary to develop a centre for the determination of critically important information entities of the enemy, including how to eliminate them physically, and how to conduct electronic warfare, psychological warfare, systemic counterpropaganda, and net operations to include hacker training”

1.2.3.2 La guerre de l'information au niveau technique

Cette guerre de l'information est menée sur le champ de bataille et consiste à obtenir l'accès total aux informations, tout en empêchant l'adversaire de faire de même[22]. L'objectif n'est pas de contrôler la signification de l'information diffusée largement, sauf dans le cas où celle-ci peut influer sur les décisions de l'ennemi, mais de conserver l'accès à celle-ci tout en utilisant une large gamme de moyens d'action pour empêcher l'adversaire de bénéficier du même avantage. Les opérations de sabotage, la lutte informatique offensive, la guerre électronique, sont les moyens principaux pour obtenir la domination de l'information sur le champ de bataille. Alors que les forces militaires en charge de la guerre électronique n'ont pas fait l'objet d'un changement majeur suite à 2008, les autorités russes ont décidé de mettre en place des troupes pouvant officiellement effectuer des opérations de lutte informatique dans le cadre d'opérations militaires. Selon Keir Giles, le conflit en Géorgie a été le point de départ du développement de forces cyber dédiées[23] et de la création cinq ans plus tard, fin 2013, d'un Cyber Command russe coordonnant la lutte informatique.

1.3 Les différents degrés d'emploi des capacités de lutte informatique dans les conflits actuels

Les capacités de lutte informatique russes ont connus une forte montée en puissance. En 2010, année de la création du Cyber Command américain, le général Alexander déclarait que ces capacités étaient très proches de celles des Etats-Unis[24]. A l'image de plusieurs Etats ayant fait un choix similaire, la Russie a rapproché au sein de ses services les capacités cyber offensives et de renseignement d'origine électromagnétique afin de maximiser leur synergie. Au moins trois cyber

[21] BBC: “Russia is underestimating information resources and losing out to the West”, Novyy Region, 29 Octobre 2008
[22] http://www.trinity.edu/rjensen/infowar.pdf
[23] http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf
[24] http://connection.ebscohost.com/c/articles/55118909/cyber-threat-pentagon-global-china-russia-near-peers-u-s

attaques majeures ont été attribuées à la Russie au cours des quinze dernières années : l'opération Moonlight Maze de 1999, l'attaque contre l'Estonie en 2007 et contre la Géorgie de 2008. Si les campagnes de cyber espionnage massives menées par des groupes de cybercriminels russes se poursuivent, et peuvent être dans une certaine mesure des "proxies" au service des intérêts russes, les capacités de lutte informatique russes ont été démontrées à différents niveaux d'intensité depuis 1999.

1.3.1 *Un vaste réseau de cybercriminels aux objectifs ciblés*

De nombreux réseaux cybercriminels russes sont capables de mener des campagnes de cyber espionnage massives et sophistiquées. Si Russian Business Network est le réseau le plus visible du fait de sa participation au conflit géorgien en 2008, d'autres groupes mènent des attaques ciblées contre des institutions officielles ou des industries stratégiques afin de collecter des données sensibles. Deux attaques attribuées à la Russie ont eu lieu contre les installations militaires américaines. La première, baptisée opération Moonlight Maze[25], a permis aux assaillants de pénétrer les réseaux internes du Pentagone, ainsi que le réseau non confidentiel du département de l'énergie américain relatif au nucléaire. Une seconde attaque contre le U.S Military Central Command en 2008 par le virus Agent.BTZ aurait également permis de collecter un grand nombre d'informations militaires sensibles[26].

Des campagnes de cyber espionnage massives et sophistiquées visant à collecter des informations sensibles ont également été lancées par des groupes de hackers russes. L'opération Red October[27] lancée en 2007 et découverte en 2013 avait pour but de collecter des données sensibles en pénétrant les systèmes d'information d'organisations gouvernementales, diplomatiques, et de laboratoires de recherche principalement en Europe, en Asie centrale et en Amérique du nord. Une seconde campagne de cyber espionnage a été découverte en 2014. Baptisée "Snake", "Ouroboros" ou "Turla", celle-ci visait les pays d'Europe de l'Ouest avec en premier lieu l'Ukraine. Il est intéressant de noter que l'intensification de cette campagne contre des cibles russes coïncident avec le début de la crise Ukrainienne comme le montre le rapport de BAE Systems[28].

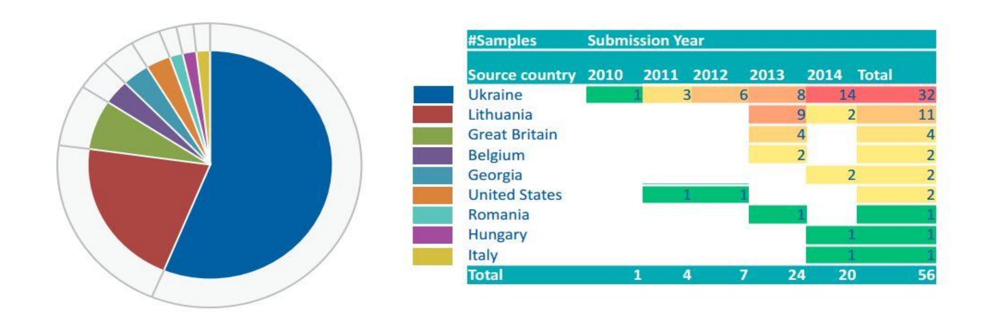
---

[25]http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php

[26]http://www.reuters.com/article/2014/03/12/us-russia-cyberespionage-idUSBREA2B25R20140312

[27]http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide

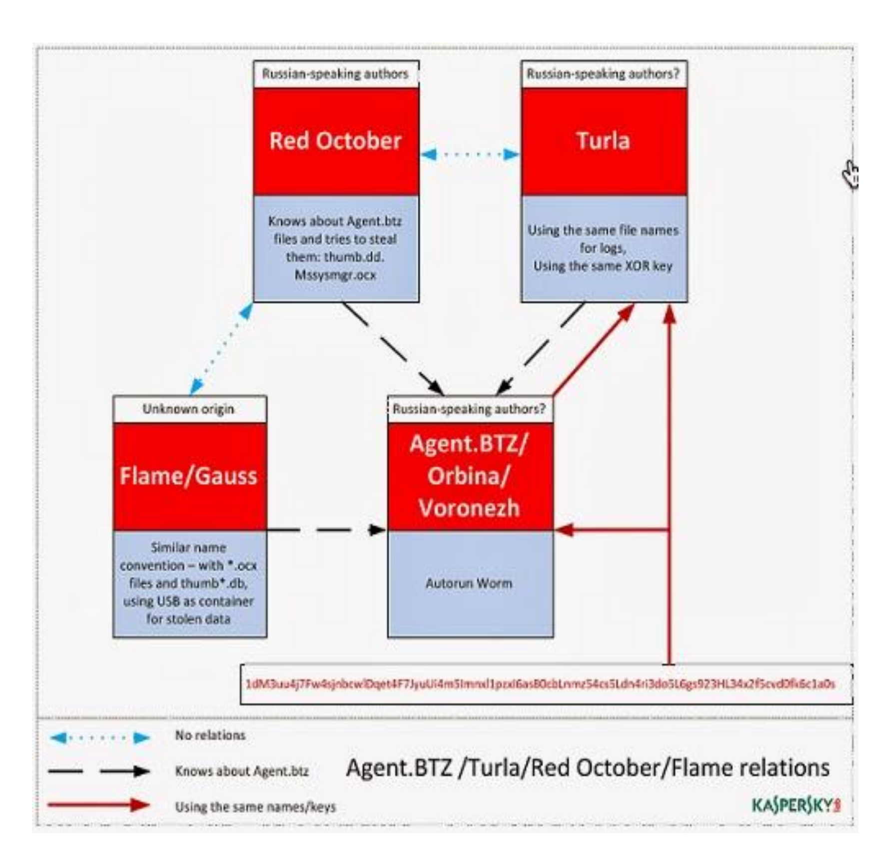
[28]http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf



#Samples	Submission Year					
Source country	2010	2011	2012	2013	2014	Total
Ukraine	1	3	6	8	14	32
Lithuania				9	2	11
Great Britain				4		4
Belgium				2		2
Georgia					2	2
United States		1	1			2
Romania				1		1
Hungary					1	1
Italy					1	1
Total	1	4	7	24	20	56

Pays les plus touchés par la campagne de cyber espionnage massives, en intensité et en fonction du temps. Source : BAE Systems[29]

Il est également intéressant de noter que des liens existent entre ces différentes campagnes, au-delà de la langue supposée des attaquants. Plusieurs similitudes dans la conception des logiciels malveillants ont permis aux chercheurs de Kaspersky de mettre en lien les différentes campagnes précédemment décrites.



Liens entre les différentes campagnes d'espionnage. Source: Kaspersky Lab[30]

[29]http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

Un autre groupe de hackers russes, sans lien apparent avec les autres campagnes de cyber espionnage, se concentre sur le secteur de l'énergie aux Etats-Unis, au Japon et dans différents pays européens. Baptisé Energetic Bear, celui-ci a pour but de s'infiltrer dans les systèmes d'information pour collecter des informations sur leur structure, les contrats en cours et les systèmes de contrôle industriels utilisés.

En dehors de Moonlight Maze et Agent BTZ, les campagnes de cyber espionnage massives n'ont pas clairement été attribuées au gouvernement russe. Cependant, les liens existant entre les campagnes, la nature des informations collectées et les systèmes d'information ciblés en priorité peuvent laisser penser que les autorités russes manifestent a minima un intérêt pour le résultat de ces campagnes sans pour autant nécessairement les coordonner à l'origine. Sans les intégrer aux opérations de lutte informatique russes, ces campagnes peuvent jouer un rôle important dans la préparation de cyberattaques massives ou dans le recueil de renseignement stratégique pour les intérêts russes.

1.3.2 *L'emploi des capacités de lutte informatique offensives dans les opérations non militaires*

Les capacités de lutte informatique russes peuvent être utilisées en dehors du cadre des opérations militaires, afin d'exercer une pression sur un État sans pour autant avoir recours aux forces cinétiques. Sans que l'attaque n'ait pu être clairement attribuée au gouvernement russe, la DDoS massive qu'a subi l'Estonie en 2007 suite à sa volonté de déplacer la statue du soldat de bronze témoigne de la pression qui peut être exercée sur un pays en utilisant des moyens de lutte informatique offensive. L'économie estonienne reposant en grande partie sur le numérique a souffert de l'attaque qui a été revendiquée par un groupe de nationalistes russes[31]. Cette capacité de pression s'est confirmée en 2008 en Géorgie, par le biais de groupes de cybercriminels russes voulant cette fois soutenir les opérations militaires russes.

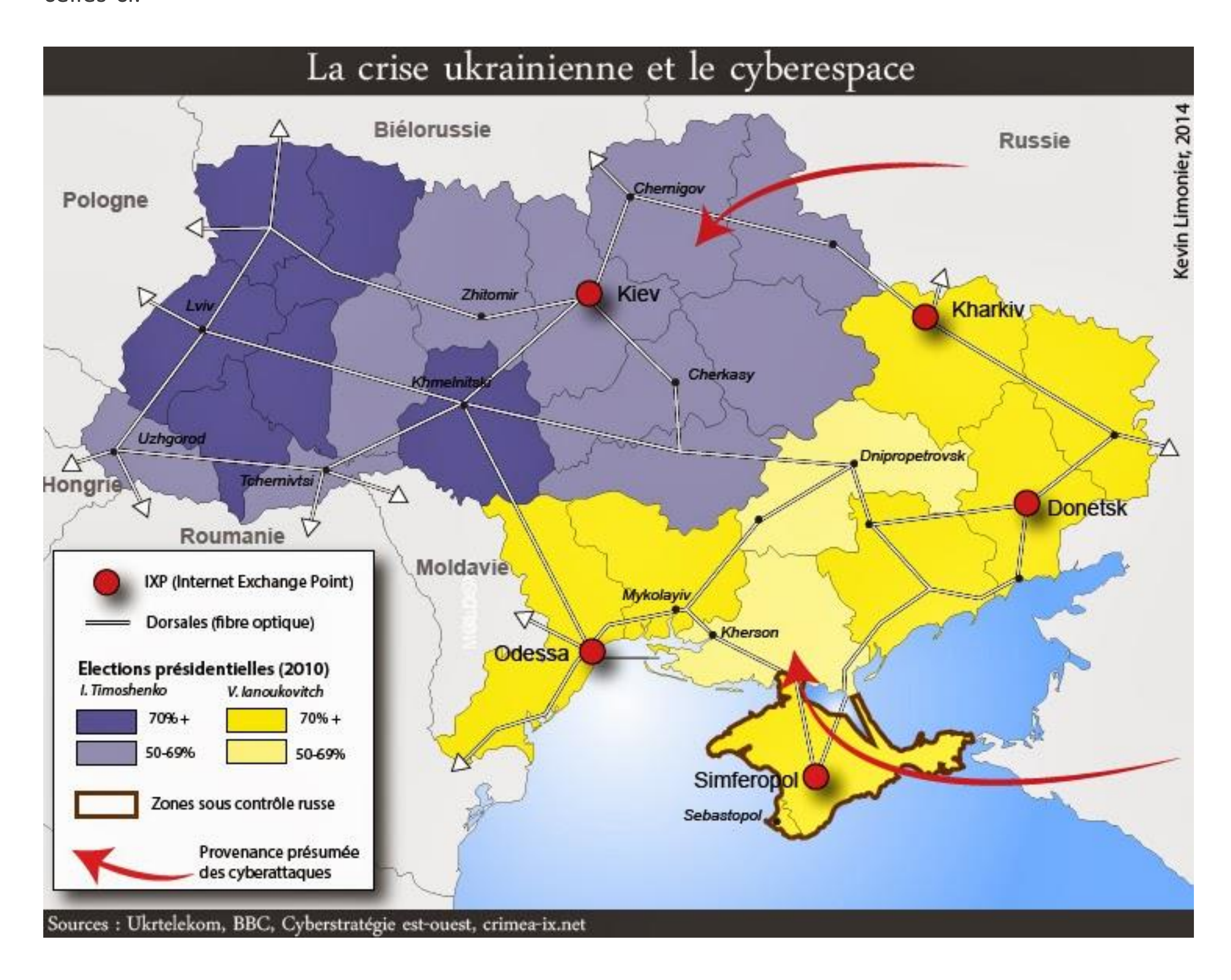
1.3.3 *L'emploi des capacités de lutte informatique offensives dans le cadre d'opérations militaires*

Alors que les opérations militaires en Géorgie en 2008 étaient appuyées par des groupes non-étatiques lançant des DDoS sur les systèmes gouvernementaux géorgiens, la crise en Ukraine de début 2014 est marquée par l'absence du même dispositif. Si plusieurs DDoS ont été lancées contre certains sites Internet de l'OTAN dont celui de son centre d'excellence, le CCDCOE, celles-ci restent d'une faible intensité et n'ont pas frappé les institutions ukrainiennes comme ce fut le cas en Géorgie.

---

[30]http://www.securelist.com/en/blog/8191/Agent_btz_a_source_of_inspiration
[31]http://www.theguardian.com/world/2007/may/17/topstories3.russia

Pourtant, la force des attaques DDoS a largement augmenté depuis 2008, ainsi que la fréquence à laquelle elles sont utilisées. Le fait qu'elles restent limitées à l'heure actuelle montre que la Russie exerce dans une certaine mesure un contrôle sur les groupes de cyber criminels qui avaient appuyé les opérations en 2008, et que ceux-ci ne l'avaient pas fait entièrement de leur propre initiative. La faible présence de ces groupes de cybercriminels et la vigueur de la campagne de cyber espionnage Snake contre les institutions ukrainiennes par rapport à d'autres pays montrent à la fois un plus fort contrôle des autorités russes sur leurs capacités cyber, ainsi qu'une augmentation qualitative de celles-ci.



Les DDoS massives de 2007 et 2008, en appui ou non des opérations militaires, ne représentent pas une constante dans les conflits modernes menés par la Russie comme le prouve la situation actuelle en Ukraine.

2. Cyberespace et milieu maritime

Considérés comme deux « espaces stratégiques communs », le cyberespace et le milieu maritime font souvent l'objet de comparaisons théoriques, par exemple pour élaborer un futur régime juridique international du cyberespace. En revanche, au plan opérationnel, les liens, pourtant nombreux, entre les deux environnements sont encore rarement évoqués.

2.1 Les systèmes d'information ont envahi le milieu maritime

Environnement transverse, le cyberespace s'incarne très directement dans le milieu maritime, comme dans les autres milieux physiques. Les réseaux informatiques et systèmes d'information ont ainsi envahi le milieu maritime. Un nouveau terme a même été créé pour décrire le phénomène : la « marétique », définie comme « *l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes, fluviales et portuaires* » dans le livre bleu publié sur le sujet en 2012 par le cluster Marétique[32].

Recelant de fantastiques opportunités, cette pénétration du maritime par le cyberespace se traduit en corollaire par l'apparition de nouveaux risques en matière de sécurité. Des risques encore très peu pris en compte, selon la plupart des observateurs du domaine. L'ENISA, l'agence de sécurité informatique de l'Union européenne, soulignait ainsi en 2011 dans un rapport sur la cybersécurité maritime[33] que la sensibilité du secteur au sujet était « faible à inexistante ». Deux faiblesses majeures étaient observées : « *les standards, méthodologies et outils dédiés à la sécurité maritime sont monolithiques et se focalisent uniquement sur la sécurité physique.* » De fait, si le livre bleu sur la « marétique » évoque à de multiples reprises l'impérieuse nécessité d'assurer la sécurité des personnes et des équipements, rien n'est dit sur la sécurité des systèmes d'information.

2.1.1 *Point sensible n°1 : les automates à bord des navires*

Ces risques portent tout d'abord sur ce que l'on appelle parfois « l'informatique enfouie » (ou embarquée), c'est-à-dire sur tous les systèmes industriels et automates que comptent les navires. Pour les marines militaires, ces dispositifs sont omniprésents dans les systèmes de combat (radar, canon, missiles…) ou les systèmes de gestion de plateforme (propulsion, électricité, fluides…). Une frégate FREMM comporte ainsi un système intégré de commande et de conduite entièrement

---

[32] http://issuu.com/opteam/docs/seagital-livre-bleu-12112013

[33] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1

équipé d'automatismes Siemens (Simatic S7-300). Dans le cas d'un navire civil, les systèmes de combat sont remplacés par des systèmes « métiers » qui jouent un rôle tout aussi clé. Exemple : le système de gestion de la charge utile dans un super tanker.

Or il est désormais de notoriété publique que ces systèmes, et notamment les Operating System, temps réel qu'ils mettent en œuvre, présentent souvent des vulnérabilités. Un institut américain spécialisé dans les transports, le Volpe Center a récemment publié une étude[34] sur la sécurité de ces systèmes. Quatre conclusions sans appel : ces systèmes sont omniprésents ; ils présentent des vulnérabilités connues ; les incidents peuvent prendre différentes formes (désactivation de certains systèmes à bord des bateaux, indisponibilité de terminaux portuaires…) ; la compromission d'un seul de ces système peut avoir des conséquences sur l'ensemble de la chaîne d'approvisionnement.

Outre « l'insider » qui injecte un code malveillant directement sur le système, le risque principal réside dans le processus de maintien en conditions opérationnelles (MCO), lequel peut être lancé au port mais aussi de plus en plus en mer. Que la mise à jour des systèmes se fasse au port, via un opérateur qui connecte son propre portable sur le système critique, ou en mer via connexion satellite, le problème sera souvent le même : aucune vérification d'intégrité n'est généralement effectuée pour s'assurer de l'innocuité du code qui est installé. La solution technique est pourtant simple, même si elle s'avère relativement onéreuse et délicate à mettre en œuvre : il s'agirait d'utiliser un système de signature pour s'assurer que le code installé lors du MCO est bien le code stipulé par le fabriquant. Il conviendrait également de mettre en place un processus de maintien en conditions de sécurité (MCS) couvrant tout le cycle de vie du système depuis les phases de conception jusqu'à son exploitation.

Le télédiagnostic et la maintenance à distance qui se généralisent peuvent enfin présenter des risques. Un tanker aurait ainsi vu sa propulsion stoppée en pleine mer il y a quelques années en raison d'une erreur d'un sous-traitant qui souhaitait réaliser une opération de maintenance et ne disposait pas du planning de navigation à jour.

Ces vulnérabilités sont encore accrues par différents éléments :

- Au plan humain : la réduction du nombre de personnes à bord des bâtiments (96 marins sur une FREMM-2005 contre 300 sur une frégate anti-sous-marine de type F67 Tourville ; environ 25 marins pour un supertanker de type VLCC[35]) ;
- Au plan technologique : une utilisation croissante de systèmes informatiques standards et de COTS pour des raisons de coût et d'interopérabilité, ce qui génère une surface d'attaque plus étendue ;

---

[34] http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf

[35] Very Large Crude Carrier, déplaçant entre 200 000 et 300 000 tonnes de port en lourd

- Au plan technique : une interconnexion des systèmes pour des raisons de supervision et de maintenance, combinée à une connectivité satellite haut débit stable, permanente et abordable offerte par la bande KA ;
- Au plan opérationnel : l'exigence d'information temps réel partagée qui a augmenté la complexité (les systèmes « métiers » et de contrôle-commande sont parfois connectés), faute d'outils de supervision adaptés.

2.1.2 *Point sensible n°2 : les infrastructures portuaires*

Comme tous les points nodaux et autres « hubs », les infrastructures portuaires constituent un maillon très sensible. Or ces ports ne sont en général pas considérés comme des éléments d'infrastructures critiques pour ce qui relève de leurs systèmes d'information, relevait l'ENISA dans son étude de 2011. Même constat aux Etats-Unis dans une étude de juillet 2013[36] intitulée « The critical infrastructure gap : US port facilities and cyber vulnerabilities » publiée par Brookings. Un officier des Coast Guards y souligne que les ports américains n'ont pas pris la mesure du problème. « *Sur les 6 ports étudiés, seulement un a conduit un audit de vulnérabilité informatique et pas un ne dispose d'un plan d'urgence au plan informatique. Surtout, sur les 2,6 millions de dollars alloués au programme sur la sécurité des ports créé à la suite du 11 septembre, à cette date, moins de 6 millions ont été consacrés à des projets de cybersécurité* ».

Quelques attaques auraient ainsi déjà eu lieu sur les systèmes d'information de ports commerciaux. L'exemple le plus probant concerne celui d'Anvers en Belgique. Ce dernier, deuxième port européen derrière Rotterdam, a été victime en 2011[37] d'un piratage informatique orchestré par un cartel de trafiquants de drogue. L'attaque a consisté à cibler des agents portuaires par l'envoi d'un malware. Ce malware a ensuite permis de récupérer un mot de passe contrôlant l'accès au système de gestion des conteneurs du port. Grâce à cet ingénieux dispositif, les trafiquants repéraient les conteneurs potentiellement intéressants en raison de leur route, les repéraient dans les zones portuaires, puis chargeaient et déchargeaient la drogue en toute discrétion.

Une attaque sur un grand port serait en fait susceptible de désorganiser massivement toute la chaine d'approvisionnement et par voie de conséquence l'économie d'un pays. Ce risque est encore accru par la multiplicité des acteurs privés et publics intervenant dans les zones portuaires et sur leurs systèmes d'information.

---

[36] http://www.brookings.edu/~/media/research/files/papers/2013/07/02%20cyber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf

[37] http://www.lalibre.be/economie/actualite/comment-anvers-a-ete-pirate-et-s-en-est-sorti-5269e7ea35708def0d93513c

2.1.3 *Point sensible n°3 : les systèmes lié à la navigation, à son contrôle et à la sécurité nautique*

De multiples dispositifs d'aide à la navigation existent. Ils se composent de façon générale d'un segment terrestre (CROSS, sémaphores, armateurs, ports, sociétés privées…), d'un segment embarqué et d'un segment spatial.

Le plus connu est sans conteste le système de positionnement GPS. Si l'on savait que celui-ci était vulnérable au brouillage, c'est un démonstrateur d'attaque beaucoup plus intelligente qu'a réussi à développer une équipe de l'Université du Texas d'Austin[38]. Il s'agissait non seulement de brouiller le signal par une émission beaucoup plus forte que celle des satellites mais de remplacer celle-ci par des trames légèrement modifiées, conduisant un navire à se détourner de quelques degrés de sa route initiale. Les données injectées étaient par ailleurs cohérentes avec les autres instruments de bord de façon à ce que le piratage ne soit pas détecté par l'équipage.

Autre système utilisé sur toutes les mers du globe, l'AIS (Automatic Identification System) qui, à l'instar du transpondeur utilisé en aviation, fournit aux navires situés à proximité des informations relatives à l'identité du bâtiment, sa position et sa route. Le système est aujourd'hui installé sur 400 000 bateaux. Or celui-ci permet de façon native à un équipage de modifier les données concernant le navire et donc de se faire passer pour un autre. Ce type de « spoofing » AIS a d'ailleurs déjà été détecté avec un tanker battant pavillon iranien, le Ramtin[39]. Le dispositif MARINT avait détecté que le navire avait transmis un nouveau « MMSI » lors de son passage dans le Golfe d'Oman. Son numéro était désormais celui d'un tanker beaucoup plus petit nommé Hamoda K qui était au même moment sur la route de Karachi, alors même que son numéro IMO (International Maritime Organization) était le bon. Intérêt évident : masquer les activités du navire inscrit sur la liste noire de l'OFAC (Office of Foreign Asset Control).

Au-delà de cette fragilité inhérente au système lui-même, les chercheurs de Trend Micro ont présenté lors de la conférence informatique HITB à Kuala Lumpur ce qui semble relever cette fois d'une vulnérabilité informatique[40]. Un attaquant pourrait tout d'abord s'attaquer aux plateformes internet fournissant des données AIS publiques pour maquiller des données valides, modifier les détails d'un bateau (course, pays, vitesse, nom, numéro MMSI ou Maritime mobile service identity, etc.), créer de faux bateaux avec les mêmes caractéristiques, ou bien encore créer et modifier des dispositifs d'assistance à la navigation (phares, balises…). D'autres vulnérabilités auraient également été découvertes cette fois dans les protocoles utilisés par les transpondeurs AIS à abord des navires.

---

[38] http://www.youtube.com/watch?v=uR0t3SUnO1Q#t=62
[39] http://www.gizmodo.com.au/2013/10/an-iranian-oil-tanker-hacked-its-own-tracking-system-to-avoid-detection/
[40] http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-discovered-in-global-vessel-tracking-systems/

Outre ces deux systèmes, l'ECDIS (Electronic Charts Display Information System), dispositif de visualisation des cartes électroniques et d'informations qui permet de fédérer tous les éléments de positionnement (sondeurs, GPS, centrales inertielles…), la cartographie, les systèmes de communication et les systèmes de navigation automatique. Selon une récente étude de la société NCC Group[41] sur l'un des principaux produits ECDIS du marché, le système pourrait présenter certaines vulnérabilités dans son processus de Maintien en Conditions Opérationnelles (MCO). L'interconnexion des systèmes critiques de l'ECDIS et des systèmes bureautiques pourraient en effet permettre des accès non autorisés, lors d'une mise à jour. Par ailleurs, un utilisateur malveillant pourrait injecter un virus via une clé USB.

Le système ECDIS

Un système ECDIS standard fonctionne sur un ordinateur tournant sous Windows XP installé sur la passerelle. Différents capteurs y sont connectés comme le radar, le navtex (télex), l'AIS, la direction, le système de positionnement, le loch (vitesse), le sondeur, l'anémomètre, le sondeur à ulltrasons, lesquels sont souvent connectés sur le réseau privé du bateau, lui-même souvent connecté à Internet. Les cartes sont quant à elle chargés dans l'ECDIS et utilisés par le personnel naviguant pour préparer la navigation, suivre son bon déroulement, la vitesse du bateau etc. Ces cartes sont téléchargées soit directement par connexion satellite, soit manuellement via des CD-ROM.



http://www.fuerstenberg-dhg.de/index.php?id=ecdis_startseite&L=1

Les systèmes d'information des réseaux et systèmes de surveillance et de gestion du trafic maritime et portuaire, de secours et de sauvetage (CROSS, chaîne sémaphorique, dispositifs de séparation de

[41] https://www.nccgroup.com/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

trafic, gestion des plans d’eau et zones de mouillage des grands ports…) ainsi que les dispositifs de balisage constituent enfin des points sensibles.

2.2 Des stratégies et des moyens d’action « cyber » spécifiques dans le milieu maritime

Le croisement du « cyber » et du maritime implique donc la conception et la mise en œuvre de stratégies et moyens d’action spécifiques. Même si les technologies et les menaces sont souvent les mêmes, chaque milieu physique possède en effet des spécificités qu’il convient de prendre en compte au plan opérationnel[42]. Même s’il est par essence globalisant et uniformisateur, le « cyber » ne peut niveler toutes les différences entre les milieux.

2.2.1 *Au niveau stratégique*

Au plan militaire, l'aspect « cyber » des opérations aéromaritimes s'est considérablement renforcé au cours des dernières années, tandis que les flottes évoluent dans un environnement de plus en plus numérisé et interconnecté. Les capacités « cyber » développées doivent ainsi être mises en adéquation avec les missions spécifiques de la Marine, notamment dans ses aspects de sauvegarde et de projection, et tenir compte de différents éléments d’environnement spécifiques propres au milieu maritime.

Les satellites constituent tout d’abord un élément important des opérations maritimes. Ils servent de soutien entre autres pour le ciblage en cas de frappe, pour les communications, la géolocalisation. Selon le général William Shelton, commandant de l'*US Air Force and Space Command*, les satellites ont augmenté l'agilité et la rapidité de réaction des forces. La destruction d'un satellite représenterait de ce fait "une importante perte de capacité"[43]. Or, les satellites sont de plus en plus menacés par le développement de technologies qui permettent de les perturber voire de les détruire à l'aide de dispositifs de brouillage, de cyberattaques, de tirs de missile ou de lasers. Le rapport annuel du Congrès américain sur la Chine mentionnait ainsi que la commission d’enquête avait eu la quasi-certitude qu’entre 2007 et 2008 la Chine avait pénétré les ordinateurs de bord de deux satellites scientifiques américains via le réseau informatique d’une station terrestre située en Norvège. Toujours en 2007, le pays avait effectué un test de destruction sur l’un de ses propres

---

[42] http://www.st-cyr.terre.defense.gouv.fr/index.php/eng/content/download/5735/39505/file/Article%2520n%25C2%25B01%2520-%2520Chaire%2520Cyberd%25C3%25A9fense%2520-%2520.pdf&sa=U&ei=TpQ0U67wB4X00gWEs4GoDQ&ved=0CCMQFjAA&sig2=Y6_ZxiWzKkvVqJmtbzx_HQ&usg=AFQjCNF6EA9X7MSoElEM8R9Qp-r_IljVvg

[43] http://freebeacon.com/general-strategic-military-satellites-vulnerable-to-attack-in-future-space-war/

satellites (Fengyun 1C). Plus récemment enfin, c'est le lancement et l'essai réussi de trois satellites scientifiques dotés de bras mécaniques pouvant être utilisés pour s'emparer d'un satellite cible qui avait défrayé la chronique[44]. Des capacités physiques pourraient donc permettre d'atteindre le cyberespace par ce biais.

L'environnement maritime constitue ensuite un milieu physique essentiel pour l'existence et le fonctionnement du cyberespace. 95 % des communications mondiales transitent par des câbles sous-marins. Y compris, les communications militaires : à titre d'exemple, le réseau de l'US Navy NETWARCOM[45] a rapporté une perte de capacité dans certaines régions du monde suite à la coupure du câble SEA-ME-WE-3. Alors que l'on ne cesse de rappeler l'importance des enjeux maritimes au XXIème siècle, notamment dans la maîtrise des approvisionnements stratégiques, la maitrise des routes « cyber » apparait donc comme un point fondamental. Les révélations Snowden le démontrent chaque jour un peu plus.

Or ces routes sont vulnérables. En matière de sabotage, tout d'abord. Il n'existe à ce jour pas d'exemple avéré de sabotage volontaire d'un câble sous-marin. Sauf à posséder des moyens d'intervention à grande profondeur, l'accès à ces câbles n'est envisageable qu'à proximité de leurs points d'atterrissage. Seules des suspicions ont été évoquées à propos du câble « South East Asia Middle East Western Europe 4 » (SEA-ME-WE 4) lorsque des ralentissements ont été observés en mars 2013[46]. Trois plongeurs ont d'ailleurs été arrêtés pour ce sabotage présumé. L'absence de cas probant à ce jour ne doit cependant pas conduire à écarter totalement ce type de scénario à l'avenir. En matière d'interception ensuite : outre les possibilités d'interception offerte par la maitrise de certaines stations terrestres, les Etats-Unis disposent d'un sous-marin, l'USS Jimmy Carter (SSN-23), entré en service en 2005, permettant de mener des opérations sous-marines sur des fibres optiques.

On note enfin que les marines militaires sont régulièrement la cible d'attaques informatiques, tant aux Etats-Unis que dans le reste du monde. En septembre 2013, le plus large réseau non confidentiel d'ordinateurs de la Navy américaine a été piraté par un groupe « *travaillant directement pour l'Iran ou agissant avec le soutien des leaders iraniens* ». Selon le Wall Street Journal qui a révélé l'attaque, le groupe a visé le réseau de la Navy /Marine Corps en utilisant une faille de sécurité dans un des sites Internet public de la marine américaine. Bien que, selon les déclarations officielles, l'attaque n'ait pas permis aux iraniens de mettre la main sur des documents classifiés, l'attaque a néanmoins été plus étendue et plus invasive que prévue. Les Iraniens n'ayant jusqu'en septembre utilisé que des attaques par Déni de Service Distribué (DDoS) contre le gouvernement américain, les autorités avaient déclaré avoir été surprises du niveau de sophistication de l'attaque. Il aura ainsi fallu quatre

---

[44] http://www.techniques-ingenieur.fr/actualite/recherche-innovation-espace-thematique_89432/shiyan-7-le-satellite-chinois-qui-fait-polemique-article_85945/
[45] http://www.computerworld.com/s/article/9237946/Sabotage_suspected_in_Egypt_submarine_cable_cut
[46] http://siliconangle.com/blog/2013/03/28/egypt-arrests-divers-trying-to-sabotage-undersea-cables/

mois pour que les équipes du Navy Cyber Command parviennent à purger le réseau de toute infection.

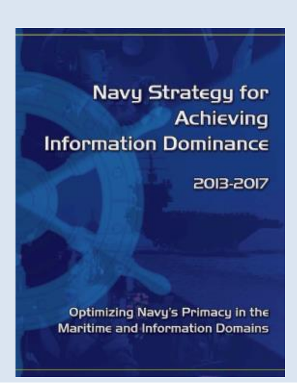
Focus sur la stratégie « cyber » de la marine américaine

Deux documents stratégiques publiés en 2012 présentent la stratégie « cyber » américaine dans le domaine naval : « Navy Cyber power 2020 »[47] et « The Navy Strategy for Achieving Information Dominance 2013-2017 »[48].

Ces documents définissent trois priorités en termes d'objectifs :

- Garantir l'accès au cyberespace et la résilience des capacités C2,
- Prévenir toute « surprise stratégique » dans le domaine par des activités de renseignement et d'analyse,
- Fournir des effets « cyber » dans le cadre des opérations militaires.





2.2.2 *Au niveau opérationnel*

Au plan opérationnel, plusieurs priorités apparaissent :

- Le **renforcement**, grâce à des actions de sensibilisation permanentes et à la responsabilisation des acteurs, des pratiques en matière d'hygiène numérique. La propagation du virus Confiker en février 2009 qui a mis à mal la disponibilité du réseau Intramar résultait d'une négligence due à un manque de sensibilisation, non d'une attaque délibérée.

- Le **développement** des formations et initiations à la sécurité informatique et à la cyberdéfense dans tous les cursus, techniques ou non techniques. Les écoles de l'enseignement maritime

[47] http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf
[48] http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Strategy_for_Achieving_Information_Dominance.pdf

pourraient ainsi disposer de modules de cybersécurité des systèmes industriels et des systèmes de navigation.

- **L'organisation d'exercices** réguliers spécifiques ainsi que l'intégration d'une composante « cyber » dans les exercices traditionnels.

- La **prise en compte d'une couche « cyber »** dans les dispositifs de surveillance et de contrôle des approches maritimes. Le système SPATIONAV, permettant la tenue à jour et le partage d'une situation des approches maritimes (SAM), implique non seulement des échanges de données entre différents services et administrations (Marine Nationale, Affaires Maritimes, Douanes, Gendarmerie…) mais également, à terme, avec les pays riverains voisins. Ce qui multiplie de facto les vulnérabilités potentielles.

- La **définition des normes et standards**, notamment en matière de maintien en conditions de sécurité (MCS), défini comme l'ensemble des actions de maintenance préventive et corrective menées sur les systèmes numériques. L'ENISA recommande ainsi une approche par les risques permettant d'évaluer la criticité des processus, l'identification des actifs, l'exposition aux risques etc. Toute la difficulté vient en fait de la gouvernance fragmentée de l'espace maritime qui se traduit, en matière de cybersécurité, par un manque de coordination et de moyens, et une multiplicité d'acteurs au plan global (International Maritime Organisation, World Customs organisation, bureau maritime international de l'ICC, International Maritime Security Corporation), et au plan européen. Des standards émergent cependant. L'United Kingdom Hydrographic Office a ainsi publié des standards de sécurité de l'information et de chiffrement (S-3) concernant les systèmes de diffusion de cartographie de navigation avec certains distributeurs. Cela a notamment été implémenté dans leur charte de service ADMIRALTY et est aujourd'hui appliqué par certains fabricants de systèmes ECDIS afin de s'assurer, grâce à un système d'authentification, de la provenance des données cartographiques. Sur ce point particulier des données hydrographiques numériques, le Service hydrographique et océanographique de la marine (SHOM) pourrait également jouer un rôle au regard de sa mission de service public au bénéfice de tous les usagers de la mer.

La mise en œuvre de ces priorités milite enfin pour la mise en place de quelques moyens spécifiques auprès de chaque commandement opérationnel. S'il ne s'agit pas de disposer, à l'instar du Cyber Command américain de structures complètes dupliquées dans chaque composante, il importe de tenir compte de la spécificité du milieu et d'avoir une structure d'animation et de coordination légère. La prochaine création d'une chaire de cybersécurité à l'Ecole Navale avec le soutien de Thales et de DCNS va dans ce sens.